M-1.5

LARA'S COMMENTS ON THE
30 OCT CIA DCID RESPONSE

In the response, CIA took ten "positions." That is, there were ten items they brought up as matters that needed resolution. A VERY condensed statement of the positions, with my comments attached, follows.

Position	Comment
1. DCID blends policy and implementation.	This is, more or less, a style issue. We probably do have too much implementation for CIA's taste or needs. However, we may have too little for the needs of many other implementors.
2. Accreditation authority should be delegated further (to the DD's at CIA.)	This issue will have to be settled above my pay grade. It is probably not solvable by the IHC, and may take DDCI resolution.
3. Data Owners should [explicitly] have input [in the accreditation process] to state protection requirements.	We agree. We assumed that the data owners would have substantial input to the accreditation process. If it needs to be explicitly stated, I see no reason not to do so.
4. CIA Deputy Directors should be able to re-delegate reaccreditation authority.	I disagree strongly. The matter of the levels of accrediting authority was thrashed out at length in the review meetings. NSA feels that System-High and Dedicated should not be delegated, let alone Compartmented mode. There aren't that many Compartmented mode systems; so, accreditation (or re-accreditation) will not be an overwhelming load and does not need further delegation.
5. The DCID should, more strongly, state that accreditation is an assumption of risk.	We thought it did. If it needs strengthening, let's do it.

CONFIDENTIAL

6. Feels that the DCID mandates the use of EPL products. Don't feel that the escape clauses are strong enough. Feel that CIA DD's should be able to "certify" systems.	Disagree. We put the term: "where feasible" in to placate NCSC and CIA (who wanted to mandate EPL products, at that time. Come what may, only the NCSC will be able to "certify" trusted systems.
7. Interim approval to operate should not be limited to one year.	Disagree. Many IC systems have been operating on interim approvals for their entire life cycle.
8. Editorial.	Unfortunate typo.
9. Media containers should be labelled only with the level of data that are expected to be put on the medium, not with the labels for all data that might be written there, deliberately or not.	Disagree. Unless the system can be trusted to not make a mistake in the kind of data written to the medium, we must assume that all output media have been contaminated with all kinds of data that are on the system.
10. Don't feel that a manual review of output classification markings is necessary, unless information is being disseminated outside the security control of the AIS facility.	Misunderstanding. We meant to say that a manual review is necessary before downgrading the output.

Agree; but give them an out

up para 35

(27)

CONFIDENTIAL